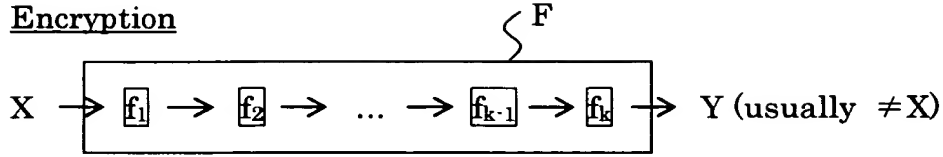


DIAGRAM



[Shimizu et al.]

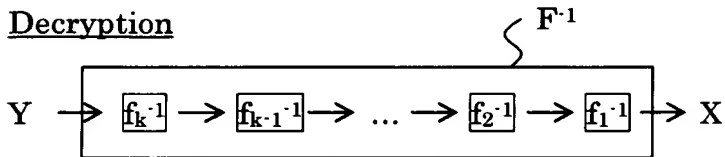
Encryption



$$F = f_k \cdot f_{k-1} \cdot \dots \cdot f_2 \cdot f_1$$

$$Y = F(X) = f_k \cdot f_{k-1} \cdot \dots \cdot f_2 \cdot f_1 (X)$$

Decryption



$$F^{-1} = f_1^{-1} \cdot f_2^{-1} \cdot \dots \cdot f_{k-1}^{-1} \cdot f_k^{-1}$$

$$X = F^{-1}(Y) = f_1^{-1} \cdot f_2^{-1} \cdot \dots \cdot f_{k-1}^{-1} \cdot f_k^{-1} (Y)$$

If f is an involution type, i.e., $f_k^{-1} = f_k, f_{k-1}^{-1} = f_{k-1}, \dots, f_2^{-1} = f_2, \dots, f_1^{-1} = f_1$,

$$F^{-1} = f_1 \cdot f_2 \cdot \dots \cdot f_{k-1} \cdot f_k$$

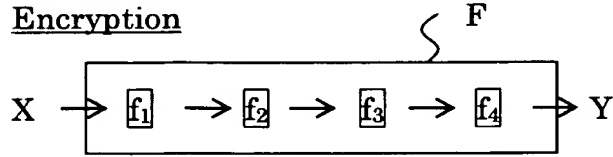
$$X = F^{-1}(Y) = f_1 \cdot f_2 \cdot \dots \cdot f_{k-1} \cdot f_k (Y)$$

DIAGRAM



[Present Invention]

Encryption



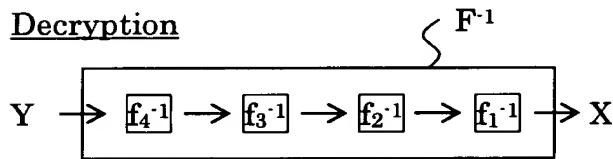
$$F = f_4 \cdot f_3 \cdot f_2 \cdot f_1$$

$$Y = F(X) = f_4 \cdot f_3 \cdot f_2 \cdot f_1(X)$$

$$\text{If } f_4 = f_1^{-1} \text{ and } f_3 = f_2^{-1}, f_2^{-1} \cdot f_2 = 1 \text{ and } f_1^{-1} \cdot f_1 = 1$$

$$Y = F(X) = f_4 \cdot f_3 \cdot f_2 \cdot f_1(X) = f_1^{-1} \cdot f_2^{-1} \cdot f_2 \cdot f_1(X) = f_1^{-1} \cdot f_1(X) = X$$

Decryption



$$F^{-1} = f_1^{-1} \cdot f_2^{-1} \cdot f_3^{-1} \cdot f_4^{-1}$$

$$X = F^{-1}(Y) = f_1^{-1} \cdot f_2^{-1} \cdot f_3^{-1} \cdot f_4^{-1}(Y) = f_4 \cdot f_3 \cdot f_2 \cdot f_1(Y) = f_4 \cdot f_4^{-1}(Y) = Y$$